REMARKS/ARGUMENTS

This Amendment is in response to the Office Action of October 4, 2005, in which the Examiner rejected all pending claims (claims 1-26). Claims 12, 21 and 26 were rejected under 35 U.S.C. 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter. Claims 1-8, 11-13 and 17-26 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,069,866 ("**Yang**") in view of U.S. Publication No. 2001/0052083 ("**Willins**"). Claims 9-10 and 14-16 were rejected under 35 U.S.C. 103(a) as being unpatentable over **Yang** in view of **Willins**, further in view of Public Key Cryptography for Initial Authentication in Kerberos, Internet Draft ("**Tung**").

By the present Amendment, Applicant has amended claims 12, 21 and 26 in order to overcome the rejection of those claims under 35 U.S.C. 112, has cancelled claim 4, has amended independent claims 1, 18, and 22 to clarify the subject matter so as to be more clearly distinguishable from the cited references, has added new claim 27, and has amended claims 5 and 7 for consistency with other claim amendments.

As recited in the claims and as described in the specification, Applicant's invention is a method and system for detecting clones (unauthorized duplicate identities) in a communications network. The method and system marks or flags an entity requesting access (having a duplicate identifier) if that entity requests access during a predetermined time or duration after a client has requested access. As recited in amended claim 1, the method includes steps such as forwarding a first signal from a client to a KDC to request access to a server, verifying that the client is authorized to access the server, transmitting a ticket (that is valid for a time T) from the KDC to the client for providing access to the server, receiving a second signal (requesting access to the server) from an entity that has identifying information identical to the client, and if the second request is prior to the expiration of the time T, marking the entity as a possible clone for further investigation while granting the entity access to the server.

Various other claims (independent claims 13 and 22 and dependent claim 27) recite further that access is subsequently denied (after investigation) if the requests from the entity (possible clone) exceed a predetermined number during the time T.

As mentioned in the specification, a suspected clone is purposely not denied access when it provides a duplicate identifier. Rather, the request could be from an authorized client that has lost its ticket and needs a new ticket for authenticating access. The marking or flagging step permits the entity to be further investigated. For example, if repeated requests come from the entity, then the entity is probably a clone, and the clone can thereafter be denied access. See paragraphs 14, 33, 34, 44, and 48-50 of the specification.

None of the cited references disclose of suggest, either alone or as combined, Applicant's invention as now recited in claim 1.

Yang discloses a system where mobile units 66 register for sessions with base stations 53 and a host computer 60. The system could go into lock-up if one mobile unit erroneously provides the same ID as another mobile unit (e.g., from a programming error or a corruption of signals during transmission -- see col. 2, lines 6-19). The system enters a mobile unit ID into a table 340 when initially requesting a session, and if another mobile unit erroneously provides the same ID, the duplication is detected and the registration is refused (see col. 6, lines 6-42). Unlike the present invention , **Yang** marks or stores the ID of the first mobile station communicating with the system. **Yang** does not "mark" an entity from which a second request is received (rather than being marked, that entity simply has access refused). In particular, **Yang** does not disclose a system wherein "if the second request is received prior to the expiration of the time T, marking the entity as a possible clone for further investigation while granting the entity access to the server" (emphasis is added), as now recited in claim 1. To the contrary, **Yang** denies access upon detection of a duplicate ID, rather than marking the entity "while granting access to the server."

Willins discloses a system where a KDC issues an electronic ticket that can be printed at a printer 222 and subsequently used to authenticate a user at a public terminal 224 for access to an application server 208 (see paragraphs 89-99). The ticket has a time stamp that is used by the system to determine when a session should end (paragraph 99). However, **Willins** does not disclose or suggest various features of the invention that are recited, for example, in claim 1. For example, **Willins** does not disclose the step of " receiving a second signal from an entity, the second signal for requesting access to the server, wherein the entity has identifying

information identical to the client," or the step of "marking the entity as a possible clone for further investigation while granting access to the server."

While the Examiner attempts to combine **Yang** with **Willins** to show Applicant's invention, Applicant believes such combination (if it could be made) (1) fails to suggest the invention because neither reference discloses several features of claim 1 (see comments above), (2) the references actually teach away from the invention, and (3) the references as combined would defeat the purpose of Applicant's invention.

In particular, if one were to combine **Yang** and **Willins** as suggested by the Examiner (assuming such combination were proper), it would show no more than a system for issuing tickets for authenticating access (**Willins**), where access is denied to a second entity if it has an ID that is identical to an earlier ID (**Yates**). As recited, e.g., in claim 1, Applicant's invention does not deny access upon receipt of a duplicate ID, but rather grants access and "marks" the requesting entity for further investigation. As recited in other claims (e.g., claims 13, 18, 22 and 27), access is denied only if an entity has been marked or flagged and upon further investigation (e.g., repeated requests with a duplicate ID from the possible clone), and the requesting entity has been determined to be a probable clone. The purported combination of **Yang** and **Willins** that teaches denying access upon receipt of a duplicate ID thus teaches away from these just-mentioned features.

In addition, as stated in the specification, the purpose of the invention is to mark suspected clones, but it is further stated that a second request with a duplicate client ID may be legitimate (e.g., because of a lost ticket). Thus as recited in claim 1, access is granted when a requesting entity is flagged (also, see for example, the specification at paragraphs 14, 44 and 48). Denying access upon receipt of a duplicate ID (as suggested by **Yates**) would defeat this purpose.

Tung discloses Kerberos-secured services using Diffie-Hellman keys. But it likewise does not disclose various other features of Applicant's invention as recited, e.g., in claim 1 (and that are referenced above).

Independent claims 13, 18 and 22 recite features similar to claim 1, are likewise distinguishable from the cited references.

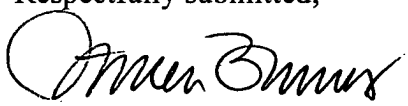
The dependent claims 2, 3, 5-12, 14-17, 19-21, and 23-27 recite limitations in addition to those of their respective parent claims and are believed allowable for the same reasons as stated above.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,



Stephen F. Jewett
Reg. No. 27,565

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300
SFJ:bhr
60615890 v1